UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

IN RE: GRAND JURY SUBPOENA
SUBPOENA TO FACEBOOK

----------X

----------X

IN RE: SUBPOENA

----------X

MEMORANDUM AND ORDER

16-MC-1300 (JO) 16-MC-1301 (JO)

16-MC-1302 (JO) 16-MC-1303 (JO)
16-MC-1304 (JO) 16-MC-1305 (JO)
16-MC-1306 (JO) 16-MC-1307 (JO)
16-MC-1308 (JO) 16-MC-1309 (JO)
16-MC-1310 (JO) 16-MC-1311 (JO)
16-MC-1312 (JO) 16-MC-1313 (JO)
16-MC-1314 (JO)

James Orenstein, Magistrate Judge:

In my role as the Duty Magistrate Judge for May 10, 2016, *see* Rules for the Division of Business Among District Judges for the Eastern District of New York 50.5(b), I have received fifteen separate applications, each with one of the two captions set forth above, each submitted in hard copy by hand but not yet filed on the court's docket, and each seeking an order pursuant to 18 U.S.C. § 2705(b) commanding the recipient of a subpoena not to disclose the subpoena's existence to any person. In each case, the application relies on a boilerplate recitation of need that includes no particularized information about the underlying criminal investigation. For the reasons set forth below, I now deny each application without prejudice to renewal upon a more particularized showing of need sufficient to support a finding that disclosure of the existence of a given subpoena will result in any of the harms that the pertinent statute lists as a basis for such a restraint.

I. Background

A. Authority to Issue Non-Disclosure Orders

The Stored Communications Act, 18 U.S.C. § 2701, *et seq.* (the "SCA"), authorizes a court, under certain defined conditions, to prohibit providers of electronic communications and remote computing services (collectively, "service providers") from notifying others of the existence of various types of government-issued orders compelling the disclosure of records. Specifically:

> The court shall enter such an order *if it determines* that there is reason to believe that notification of the existence of the warrant, subpoena, or court order *will* result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b) (emphasis added).

B. The Government's Applications

1. *In re: Subpoena*

In each of the *In re: Subpoena* ("*Subpoena*") actions, the government has filed under seal a motion styled as follows: "APPLICATION FOR ORDER COMMANDING [SERVICE PROVIDER] NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF SUBPOENA[.]" The text of each application is identical, save for the identification of the service provider that is the subject of the proposed order. I reproduce below the application's full text.[1]

> The United States requests that the Court order [service provider] not to notify any person (including the subscribers and customers of the accounts(s) listed in the subpoena) of the existence of the attached subpoena until further order of the Court.
>
> [Service provider] is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached subpoena, which requires [service provider] to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.*

[1] The application in each case includes a copy of the pertinent grand jury subpoena as an attachment; it should therefore remain under seal. There is nothing in the quoted text of the application, however, that will reveal anything about the government's investigation.

> In this case, such an order would be appropriate because the attached subpoena relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure *may* alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached subpoena *will* seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, and/or change patterns of behavior. *See* 18 U.S.C. § 2705(b). Some of the evidence in this investigation is stored electronically. If alerted to the existence of the subpoena, the subjects under investigation *could* destroy that evidence.
>
> WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing [service provider] not to disclose the existence or content of the attached subpoena, except that [service provider] may disclose the attached subpoena to an attorney for [service provider] for the purpose of receiving legal advice.
>
> The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Subpoena, Application at 1-2 (emphasis added).

On the basis of that application, the government in each case asks me to enter the following order:

> The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding [service provider], an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the subpoena) of the existence of the attached subpoena until further order of the Court.
>
> *The Court determines* that there is reason to believe that notification of the existence of the attached subpoena *will* seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, and/or change patterns of behavior. See 18 U.S.C. § 2705(b).
>
> IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that [service provider] shall not disclose the existence of the attached subpoena, or this Order of the Court, to the listed subscriber or to any other person, unless and until otherwise authorized to do so by the Court, except that [service provider] may disclose the attached subpoena to an attorney for [service provider] for the purpose of receiving legal advice.

> IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

Subpoena, Proposed Order at 1-2 (emphasis added).

2. *In re: Grand Jury Subpoena to Facebook*

Each of the two applications captioned *In re: Grand Jury Subpoena to Facebook* ("*Facebook*") is similar to its counterparts in the *Subpoena* cases, with one exception discussed below. Each relies on the same assertions about potential investigative harms to seek an order prohibiting Facebook from disclosing the existence of the pertinent subpoena to any person, and each seeks a non-disclosure order including, in essentially the same language, the same findings and directives quoted above.[2]

In addition to seeking a non-disclosure order, the *Facebook* applications also include a request for an order prohibiting Facebook from taking certain other actions – which the government asserts Facebook has previously taken in comparable circumstances – that do not inherently reveal the existence of the subpoena but that, in the government's view, "provid[e] government targets effective notice that they are the subject of government investigation." *Facebook*, Application at 2.[3] Based on that assertion about "effective notice," the government asserts that the additional relief it seeks is authorized under the non-disclosure provision of 18 U.S.C. § 2705(b). Accordingly, the proposed order in each *Facebook* action also includes the following language:

> *The Court determines* that there is reason to believe that notification of the existence of the Subpoena or [the additional actions at issue] *would* provide targets of the

[2] The only textual difference between the two categories of applications and proposed orders that is even remotely substantive, aside from those differences that accommodate the government's additional request in *Facebook*, is that the *Facebook* applications cite subsections (2), (3), and (5) of 18 U.S.C. § 2705(b), whereas the *In re: Subpoena* applications provide no such specificity. In each case, however, the government raises concerns about the same potential harms to its investigations.

[3] As discussed below, the government has not yet provided any basis to conclude either that Facebook will take the actions at issue if not prohibited from doing so or that such actions would in any way compromise any criminal investigation. Nevertheless, because I have not previously asked the government to substantiate its assertions in this regard, I avoid a specific description of the conduct the government seeks to regulate in order to allow a public discussion of the reasons for this order.

> investigation with effective notice of *the government's investigation* and would seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. See 18 U.S.C. § 2705(b)(2), (3), (5).

Facebook, Proposed Order at 1 (emphasis added).

II. Discussion

A. Prejudice to Investigations

1. Prejudice Arising From Actual Notification of a Subpoena's Existence

As noted above, the sole fact that the government posits in each case in support of a non-disclosure order is that the pertinent subpoena "relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation[.]" Application at 1. From this premise, the government concludes that the subpoena's "disclosure *may* alert the targets to the ongoing investigation." *Id.* (emphasis added).[4] Having thus sought to demonstrate the possibility of tipping off a target to the existence of an investigation, the government then reasons that disclosure of the subpoena therefore "*will* seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, and/or change patterns of behavior." *Id.* at 1-2 (emphasis added). Moreover, the government notes that "[s]ome of the evidence in this investigation is stored electronically." *Id.* at 2. As a result, the government concludes, "[i]f alerted to the existence of the subpoena, the subjects under investigation

[4] I assume for purposes of discussion that in each case there are in fact specific "targets" of the pertinent investigations – that is, persons "as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant." U.S. Attorney's Manual § 9-11.151. It would, however, be somewhat surprising if that were true: in a great many cases – including some in which the government might have a very good reason to fear that disclosing a subpoena's existence might prejudice the government's investigation – a grand jury can subpoena and receive a great deal of information long before the government concludes that anyone qualifies as a "target" rather than a "subject" of the investigation (that is, a person whose conduct is merely "within the scope of the grand jury's investigation[,]" *id.*). The difference between a target and a subject, however, is one of some significance to consideration of the likely effect of the disclosure of a subpoena.

could destroy that evidence." *Id.* (emphasis added).[5] I respectfully disagree with the government's reasoning.

First, while it is unquestionably true that a service provider's disclosure of a subpoena for customer records "may" alert the target of an investigation to its existence, it is just as true that disclosure may not have that effect. To cite just one example, sometimes subpoenas for service providers' records seek information from the account of a target's victim (who might well fall within the definition of an investigative "subject"), or from some other person whose interests are not aligned with the target's but who may nevertheless have information relevant to the investigation. In such circumstances, there is simply no reason to presume that disclosure of the subpoena to the customer whose records the government seeks will harm the investigation in any way at all. Thus, before I can conclude that disclosure "will" result in such harm as the statute requires, I must have information about the relationship, if any, between the customer whose records are sought and any target of the investigation.[6] The sole fact asserted by the government to date – the targets' ignorance of the existence of an ongoing criminal investigation – does not support an inference that a service provider's disclosure of a subpoena to the pertinent customer will have any effect on the investigation.

---

[5] It is not clear that the government intends to posit a connection between the fact that some evidence is stored electronically and the likelihood of any of the harms listed in Section 2705(b). If that is the government's intent, it has not explained why it is any more likely for an investigative target to engage in obstructive conduct when some evidence is stored electronically than when the evidence takes other forms. If anything, the reality that electronically stored evidence is often accessible in multiple repositories (and thus harder to effectively erase) and that attempts to delete or alter such evidence (even if successful) often leave identifiable traces – facts which appear to be gaining wider dissemination in an increasingly technologically proficient society – suggests at least a possibility that tipping off a target to the existence of an investigation will pose less risk to electronically stored evidence than to physical documents or the availability of oral testimony.

[6] The government provides no reason to anticipate that the service provider in each case would notify anyone other than the customer whose records are sought. If there is reason to believe the service provider would alert persons other than the pertinent customer if not prohibited from doing so, the government can of course make such a showing.

Second, there is no reason to assume that tipping off an investigative target to the investigation's existence necessarily "will" result in one of the harms contemplated by the SCA. To be sure, such information can easily have such an effect. But if Congress presumed that providing such information to an investigative target would inevitably lead to such consequences, the judicial finding the SCA requires would be meaningless. There will plainly on occasion be circumstances in which an investigative target either lacks the ability or the incentive to flee, to tamper with evidence, or otherwise to obstruct an investigation. To cite just two possibilities: the target may be incarcerated and lack effective access to evidence and witnesses; alternatively, the target may be a public figure with a strong incentive to affect a public posture of innocence and cooperation with law enforcement. In most cases, it seems likely that the government can easily make a showing that there is reason to believe that a target's knowledge of an investigation will indeed lead to obstructive behavior – but not in every case.

In short, the government contends that notification necessarily will lead to obstruction. But the SCA precludes such reasoning; to the contrary, it allows a court to issue a non-disclosure order only "if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result[.]" 18 U.S.C. § 2705(b). That language inherently assumes that sometimes notifying the target of the existence of an investigation will result in certain types of misconduct but that other times it will not, and that it is up to a judge to make the necessary determination in a given case based on the available evidence. As a result, in the absence of any case specific information aside from the assertion that the target of an investigation does not know of its existence, it is impossible to make the factual determination necessary for a non-disclosure order.

Finally, the government's assertion that "[i]f alerted to the existence of the subpoena, the subjects under investigation *could* destroy that evidence[,]" Application at 2 (emphasis added), is

manifestly insufficient. The SCA requires a determination that disclosure "will" have certain adverse effects, not that it "could" do so.

Government prosecutors and agents have a difficult job investigating crime, and one that is made more difficult by the fact that some of the investigative techniques they must rely on can backfire by alerting criminals to the fact of the investigation.[7] The SCA provides some measure of relief against that risk, but it does not do so indiscriminately. The government cannot, consistent with the statute, obtain an order that constrains the freedom of service providers to disclose information to their customers without making a particularized showing of need. The boilerplate assertions set forth in the government's applications do not make such a showing, and I therefore deny all of the pending requests for non-disclosure orders. The ruling is without prejudice to the government's right to renew its requests on the strength of additional facts about each investigation that permit a finding that disclosure of a subpoena will result in an identifiable form of harm to the investigation.[8]

---

[7] To guard against that risk, the government routinely asks subpoena recipients who are not investigative targets to voluntarily refrain from disclosure – and also, on occasion, improperly turns that request into what appears to be a judicial command on the face of the subpoena itself. *See United States v. Gigliotti*, 15-CR-0204 (RJD), docket entry 114 (Memorandum and Order), slip op. at 2-3, 7-8 (E.D.N.Y. Dec. 23, 2015). It is entirely understandable that the government is as proactive as the law allows it to be in maintaining the secrecy of its investigations, and just as understandable that it will seek to test those legal limits. Applications for the kind of non-disclosure orders at issue here have been routinely granted for a long time, and I do not fault the government for continuing to engage in a practice that I and other judges have unquestioningly endorsed. But having belatedly reconsidered the issue, I now conclude that my prior orders granting similar boilerplate applications were erroneous.

[8] I do not consider or address here the extent to which the relief the government seeks is in tension with either the First Amendment rights of service providers to provide information to their customers or the Fourth Amendment rights of those customers to be provided notice of the government's search or seizure of their records. First, as explained above, the government has not yet established the facts necessary to support a non-disclosure order under the SCA, and so any such discussion would be premature. Second, such issues can more efficiently be resolved through adversarial testing. It is clear that a service provider subjected to a non-disclosure order under the SCA has the ability to raise such arguments in an adversarial setting after the order has issued. *See Microsoft Corp. v. U.S. Dep't of Justice*, 16-CV-0538 (JLR), docket entry 1 (Complaint) (W.D. Wash. Apr. 14, 2016) (seeking a declaration that the provision for non-disclosure orders under 18 U.S.C. § 2705(b) is unconstitutional).

2. Prejudice Arising From Facebook's Potential Additional Actions

In addition to a prohibition on explicit notification of the existence of the pertinent subpoena, each of the *Facebook* applications also seeks an order prohibiting Facebook from taking certain actions that the government asserts would indirectly, but effectively, alert targets to the existence of the government's underlying investigation. As an initial matter, this request fails for the same reasons that the request for a prohibition of explicit notification of the subpoena fails: the government has not established either that disclosure of the subpoena to a given customer will result in alerting the target to the investigation's existence or that the target of the investigation will, if notified, engage in obstructive conduct. As explained below, another reason to deny relief with respect to indirect notification is that the government has not adequately explained the connection between the actions it wants to prohibit Facebook from taking and the harm it seeks to forestall.

The government has stated no more than that Facebook has taken such actions previously in response to receiving subpoenas. *Facebook*, Application at 2. What the government has not told me is (a) whether Facebook routinely does so in response to every subpoena, or only in certain circumstances; and (b) whether, and under what circumstances, Facebook takes the same actions even in the absence of receiving a subpoena. The actions are of a sort that a service provider like Facebook might take for a wide variety of reasons having nothing to do with any criminal investigation of the customer. It therefore seems quite likely – indeed, in my view, more likely than not – that the actions at issue would not necessarily lead a Facebook customer to infer the existence of a criminal investigation, much less the existence of a subpoena.[9]

[9] In this context, the distinction between the subpoena and the underlying investigation is significant. The SCA allows a court to order a service provider "not to notify any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b). If Facebook took the actions at issue in response to any indication of a criminal investigation of a customer – including informal requests for assistance, or reports about the existence of an investigation, or allegations by other customers of criminal conduct – a customer might correctly infer from Facebook's actions the existence of an

Moreover, the government provides no authority for the proposition that the SCA authorizes a court to prohibit an action that merely allows a customer to infer the existence of a subpoena – as opposed to prohibiting actual notification of that fact. The statute does not explicitly provide such authority, and such a broad reading of the law might have adverse consequences for a service provider or others that Congress did not intend. For example, if Facebook takes the actions for its own business purposes upon learning of a subpoena as a prophylactic measure to prevent a customer suspected of criminal conduct from using Facebook's services to harm others, prohibiting it from doing so would impose burdens on Facebook and others that a prohibition on actual notification of a subpoena would not.[10] Accordingly, in the absence of legal authority for its broad reading of the SCA, as well as the absence of any factual basis for determining that Facebook's actions would themselves disclose the existence of the pertinent subpoenas, I deny the government's request to prohibit Facebook from taking certain actions.

B. Imposing Secrecy Requirements on the Recipients of Federal Grand Jury Subpoenas

The SCA provision generally authorizing a court to issue a non-disclosure order to a service provider receiving a subpoena does not differentiate among the different specific types of subpoena

---

investigation even if no subpoena existed that could serve as the predicate for a non-disclosure order. The SCA confers no authority to prohibit notification of the existence of an investigation – only "the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b). Without more information about the circumstances in which Facebook does and doesn't take the actions at issue, it is impossible to determine whether, in a given case, they would cause a customer to infer the existence of a subpoena.

[10] The government's broad reading of the SCA could also justify issuing an order requiring a service provider to make affirmatively false or misleading statements to its customers and to the public. *See generally* Wendy Everette, *"The F.B.I. Has Not Been Here (Watch Very Closely For The Removal Of This Sign)": Warrant Canaries And First Amendment Protection For Compelled Speech*, 23 Geo. Mason L. Rev. 377 (2016) (discussing the emergence of "warrant canaries" that periodically advise the public about the extent to which warrants and court orders have been served, to allow an inference of the existence of a warrant subject to a non-disclosure order if the periodic notification stops); Naomi Gilens, *The NSA Has Not Been Here: Warrant Canaries As Tools for Transparency in the Wake of the Snowden Disclosures*, 28 Harv. J.L. & Tech. 525 (2015) (same). I need not and do not consider here whether an order requiring a service provider to engage in such affirmative deception would be in tension with the First Amendment.

that a service provider might receive.[11] However, to the extent the statute provides for the issuance of an order prohibiting a service provider from disclosing the existence of a federal grand jury subpoena in particular, it is in tension with the specific rule that, as to federal grand jury proceedings, "[n]o obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B)." Fed. R. Crim. P. 6(e)(2)(A). The cited rule does not make any provision for imposing an obligation of secrecy on a witness or subpoena recipient. *See* Fed. R. Crim. P. 6(e)(2)(B); *see also* Fed. R. Crim. P. 6 advisory committee's note (1944 adoption note 2 to subdivision (e): "The rule does not impose any obligation of secrecy on witnesses.... The seal of secrecy on witnesses seems an unnecessary hardship and may lead to injustice if a witness is not permitted to make a disclosure to counsel or to an associate.").

I need not and do not resolve here the tension between the provision of the SCA allowing a court to impose a secrecy requirement on certain businesses receiving a wide array of state and federal compulsion orders and the rule specifically exempting federal grand jury witnesses from any secrecy requirement. My research to date reveals only two federal court opinions that address the matter: the two cases were decided in district courts outside of this circuit and reached opposite conclusions. *See In re Application of the U.S. For An Order Pursuant To 18 U.S.C. § 2705(b)*, 131 F. Supp. 3d 1266, 1276 (D. Utah 2015) (holding that the SCA permits the imposition of "secrecy obligations in addition to those stated in Rule 6(e)(2)"); *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2705(b)*, 866 F. Supp. 2d 1172, 1173 (C.D. Cal. 2011) (holding that because of the prohibition of additional secrecy

[11] The SCA contemplates a variety of ways in which a government entity can compel a service provider to produce records, including by means of a warrant issued by a state or federal court; an administrative subpoena issued by a state or federal agency; a state or federal grand jury subpoena, or another kind of state or federal court order. *See* 18 U.S.C. § 2703(b)(1).

requirements in Fed. R. Crim. P. 6(e)(2)(A), the SCA "cannot properly be read as authorizing the Court to enjoin a provider from revealing that it has received a grand jury subpoena").[12]

The government's failure to establish the factual assertion necessary for an order under the SCA obviates the need for such a decision now. Should the government renew its applications based on individualized evidence that disclosure of a given subpoena will result in any of the harms listed in Section 2705(b), it should be prepared to demonstrate legal authority for the imposition of a secrecy requirement on a federal grand jury witness notwithstanding the specific prohibition in Rule 6.

III. Conclusion

For the reasons set forth above, I deny the application for a non-disclosure order in each of the captioned cases without prejudice to renewal upon a particularized showing of need. I respectfully direct the Clerk to create a separate public docket for each application, and within each such docket to file the pertinent application under seal to preserve the secrecy of the underlying criminal investigation, and to file this document, unsealed, on each such docket.

SO ORDERED.

Dated: Brooklyn, New York
May 12, 2016

/s/
JAMES ORENSTEIN
U.S. Magistrate Judge

[12] In a third case, *In re Application of the United States of Am. for Nondisclosure Order Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014032122836*, 2014 WL 1775601, at *4 (D.D.C. Mar. 31, 2014), the court declined to issue a non-disclosure order without first allowing the subject of the proposed order (Twitter) to be heard. The magistrate judge's opinion did not refer explicitly to Rule 6(e)(2)(A), but did rely in part on the decision from the Central District of California cited above. *See id.* at *3. The district judge reviewing the magistrate judge's decision overruled it and issued the requested non-disclosure order. In doing so, the court noted that Rule 6(e) did not authorize seeking Twitter's input and permitted the sealing of the application and non-disclosure order; but the court did not address the applicability of Rule 6(e)(2)(A) to the viability of the government's request for a non-disclosure order under the SCA. *See Matter of Application of United States of Am. for an Order of Nondisclosure Pursuant to 18 U.S.C. §2705(B) for Grand Jury Subpoena # GJ2014031422765*, 41 F. Supp. 3d 1, 6-8 (D.D.C. 2014).